Zertifizierungsreport

Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0023-2007

zu

Schutzprofil
Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0

entwickelt im Auftrag des

Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-5477

Bundesamt für Sicherheit in der Informationstechnik

Zertifikat BSI-PP-0023-2007

Schutzprofil
Software zur Verarbeitung von personenbezogenen Bilddaten
Version 2.0

Common Criteria Vereinbarung

entwickelt im Auftrag des

Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Vertrauenswürdigkeitspaket: **EAL1**

Bonn, den 19.01.2007

Der Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik

Hange L.S.

Das oben genannte Schutzprofil wurde von einer akkreditierten und lizenzierten Prüfstelle nach den *Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3,* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik Version 2.3*, evaluiert.

Dieses Zertifikat gilt nur für die angegebene Version des Schutzprofils und nur in Verbindung mit dem vollständigen Zertifizierungsreport.

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlußfolgerungen der Prüfstelle stehen in Einklang mit den erbrachten Nachweisen.

Mit diesem Zertifikat ist weder eine generelle Empfehlung des Schutzprofils noch eine Garantie des Bundesamtes für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluß hatte, verbunden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-5477

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] neben der Zertifizierung von Sicherheitsprodukten der Informationstechnik auch die Aufgabe, Schutzprofile (PP)[2] für solche Produkte zu zertifizieren.

Ein Schutzprofil definiert eine implementierungsunabhängige Menge von IT-Sicherheitsanforderungen an eine Kategorie von Produkten (Systeme oder Komponenten). Anwender können durch Erstellung und Zertifizierung eines Schutzprofils oder Verweis auf ein solches ihre IT-Sicherheitsbedürfnisse ausdrücken, ohne Bezug auf ein konkretes Produkt zu nehmen. Schutzprofile können als Grundlage für eine Produktzertifizierung herangezogen werden. Produkte, die eine solche Zertifizierung durchlaufen haben, erhalten ein eigenes Zertifikat.

Die Zertifizierung eines Schutzprofils wird auf Veranlassung des Schutzprofil-Entwicklers - im folgenden Antragsteller genannt - durchgeführt. Entwickler eines Schutzprofils können IT-Hersteller, aber auch IT-Anwender sein.

Bestandteil des Verfahrens ist die Evaluierung (Prüfung und Bewertung) des Schutzprofils gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Evaluierung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder von der Prüfstelle des BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Schutzprofils, die Einzelheiten der Bewertung und Hinweise für den Anwender.

---

[1] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

[2] Protection Profile

Gliederung

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSIG[3]
- BSI-Zertifizierungsverordnung[4]
- BSI-Kostenverordnung[5]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)
- Verfahren der Erteilung eines PP-Zertifikats durch das BSI
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3 (ISO/IEC 15408)
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI Zertifikate: Anwendungshinweise und Interpretationen zum Schema (AIS)

---

[3] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

[4] Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) vom 7.Juli 1992, Bundesgesetzblatt I S. 1230

[5] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

2 Anerkennungsvereinbarungen

Um die Mehrfach-Entwicklung des gleichen Schutzprofils in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von Zertifikaten für Schutzprofile unter gewissen Bedingungen vereinbart.

Im Mai 2000 wurde eine Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 zwischen den nationalen Stellen in Australien, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Kanada, Neuseeland, Niederlande, Norwegen, Spanien und den USA unterzeichnet. Israel trat im November 2000 der Vereinbarung bei, Schweden im Februar 2002, Österreich im November 2002, Ungarn und Türkei im September 2003 und Japan im November 2003, die Tschechische Republik im September 2004, die Republik Singapore im März 2005, Indien im April 2005.

3 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Schutzprofil „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“ hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Schutzprofils „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“ wurde von der CSC Deutschland Solutions GmbH durchgeführt. Die CSC Deutschland Solutions GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Antragsteller ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Entwickelt wurde das Schutzprofil „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“ im Auftrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch die datenschutz nord GmbH und das BSI.

Die Entwicklung und Evaluierung des Schutzprofils wurde auf der Grundlage der CC Version 2.3 (ISO/IEC 15408), sowie der AIS durchgeführt.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 19. Januar 2007 vom BSI abgeschlossen.

[6] Information Technology Security Evaluation Facility

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-10.

Das Schutzprofil „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“ ist in die BSI-Liste der zertifizierten Schutzprofile, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Unter der o.g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

B Zertifizierungsbericht

Gliederung des Zertifizierungsberichtes

1 PP-Übersicht

Das auf den Common Criteria basierende Schutzprofil (Protection Profile – PP) „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“ thematisiert die Mindestanforderungen, die an die Software zur Verarbeitung von personenbezogenen Bilddaten gestellt werden, um einerseits den datenschutzrechtlichen Bestimmungen zu genügen und andererseits eine anwenderfreundliche Bedienung der IT-Sicherheit moderner Videoüberwachungsanlagen zu ermöglichen. Die im PP beschriebene Software zur Verarbeitung von personenbezogenen Bilddaten wird im Folgenden als Evaluierungsgegenstand (EVG) bezeichnet.

Die im Schutzprofil charakterisierte datenschutzkonforme Videoüberwachungsanlage kann Bilddaten von an den EVG angeschlossenen Signalaufnahmekomponenten empfangen und auf Authentizität (Herkunft der Daten) prüfen. Einmal gespeicherte Bilddaten stehen unter der Kontrolle des EVGs, bis sie gemäß der maximalen Aufbewahrungsfrist automatisch gelöscht werden. In dieser Zeit können über den EVG nur registrierte Benutzer auf die Bilddaten zugreifen. Abhängig von der Rolle des jeweiligen Benutzers (z.B. Beobachter oder Revisor) erlaubt der EVG den Export von Bilddaten aus dem EVG heraus oder auch das Löschen einzelner Bilddaten.

Für alle datenschutzrelevanten Benutzer-Aktionen fordert der EVG vor Durchführung der Aktion zur Eingabe einer Begründung auf, welche in den Protokolldaten gespeichert wird. Neben diesen Benutzer-Aktionen und Begründungen protokolliert der EVG auch seinen Start und seinen Stopp sowie Beginn und Ende eines Bildausfalls einer Signalaufnahmekomponente. Die Protokolldaten stehen nach der Erzeugung und Speicherung unter der Kontrolle des EVG. Der EVG ist dazu in der Lage, nicht autorisierte Manipulationen an den Protokolldaten zu erkennen.

Der hier beschriebene EVG schützt die Bilddaten erst nach dem Empfang. Die EVG-Umgebung muss dafür sorgen, dass die Bilddaten vertraulich und integer sowie authentisch (Aufnahme aus zulässigem Bereich und Kamera hat Realität erfasst) beim EVG ankommen. Weiterhin vertraut der EVG auf eine physikalisch abgesicherte Einsatzumgebung, eine korrekte Konfiguration der Hardware und auf vertrauenswürdiges Bedienpersonal.

Die softwaregestützte automatisierte Verarbeitung von Bilddaten umfasst gemäß §3 Bundesdatenschutzgesetz (BDSG) die Erhebung (also die Aufnahme), die Verarbeitung (vorrangig Speichern und Löschen) und die Nutzung (z. B. die Auswertung/Suche) von Bilddaten.

Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, entsprechen der Vertrauenswürdigkeitsstufe EAL1.

2 Funktionale Sicherheitsanforderungen

Die folgenden funktionalen Sicherheitsanforderungen aus Teil 2 der CC werden im vorliegenden Schutzprofil für den EVG definiert:

Funktionale Sicherheits-anforderungen	Bedeutung
FAU	**Sicherheitsprotokollierung**
FAU_GEN.1	Generierung der Protokolldaten
FAU_SAR.1	Durchsicht der Protokollierung
FDP	**Schutz der Benutzerdaten**
FDP_IFC.1	Teilweise Informationsflusskontrolle
FDP_IFF.1	Einfache Sicherheitsattribute
FDP_ITC.2	Import von Benutzerdaten mit Sicherheitsattributen
FDP_RIP.1	Teilweiser Schutz bei erhalten gebliebenen Informationen
FDP_SDI.1	Überwachung der Integrität der gespeicherten Daten
FIA	**Identifikation und Authentisierung**
FIA_UAU.2	Benutzerauthentisierung vor jeglicher Aktion
FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion
FMT	**Sicherheitsmanagement**
FMT_MSA.1	Management der Sicherheitsattribute
FMT_MSA.3	Initialisierung statischer Attribute
FMT_MTD.1	Management der TSF-Daten
FMT_SMF.1	Spezifikation der Managementfunktionen
FMT_SMR.1	Sicherheitsrollen
FPT	**Schutz der TSF**
FPT_TDC.1	Einfache Inter-TSF TSF-Datenkonsistenz

Tabelle 1: SFRs für den EVG

Hinweis: Es werden nur die Titel der SFRs genannt. Detailiertere Informationen befinden sich in Kapitel 5.1 des Schutzprofils [7].

Folgende funktionale Sicherheitsanforderungen aus Teil 2 der CC werden im vorliegenden Schutzprofil für die IT-Umgebung des EVGs definiert:

Funktionale Sicherheits-anforderungen	Bedeutung
FDP	**Schutz der Benutzerdaten**
FDP_ACC.2	Vollständige Zugriffskontrolle
FDP_ACF.1	Zugriffskontrolle basierend auf Sicherheitsattributen
FDP_ETC.2	Export von Benutzerdaten mit Sicherheitsattributen
FDP_IFC.1	Teilweise Informationsflusskontrolle
FDP_IFF.1	Einfache Sicherheitsattribute
FMT	**Sicherheitsmanagement**
FMT_MSA.1	Management der Sicherheitsattribute
FMT_MSA.3	Initialisierung statischer Attribute
FPT	**Schutz der TSF**
FPT_STM.1	Verlässliche Zeitstempel

Tabelle 2: SFRs für die IT-Umgebung des EVGs

3 Vertrauenswürdigkeitspaket

Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, sind in nachfolgender Tabelle aufgeführt. Sie entsprechen der Vertrauenswürdigkeitsstufe EAL 1 und der Klasse ASE für die Sicherheitsvorgaben aus Teil 3 der Common Criteria.

Vertrauenswürdigkeitsklassen und Komponenten	
ASE	**Security Target Evaluierung**
ASE_DES.1	EVG-Beschreibung
ASE_ENV.1	Sicherheitsumgebung
ASE_INT.1	ST-Einführung
ASE_OBJ.1	Sicherheitsziele
ASE_PPC.1	PP-Postulate
ASE_REQ.1	IT-Sicherheitsanforderungen
ASE_SRE.1	Explizit dargelegte IT-Sicherheitsanforderungen
ASE_TSS.1	EVG-Übersichtsspezifikation
ACM	**Konfigurationsmanagement**
ACM_CAP.1	Versionsnummern
ADO	**Auslieferung und Betrieb**
ADO_IGS.1	Installations-, Generierungs- und Anlaufprozeduren
ADV	**Entwicklung**
ADV_FSP.1	Informelle funktionale Spezifikation
ADV_RCR.1	Informeller Nachweis der Übereinstimmung
AGD	**Handbücher**
AGD_ADM.1	Systemverwalterhandbuch
AGD_USR.1	Benutzerhandbuch
ATE	**Testen**
ATE_IND.1	Unabhängiges Testen – Übereinstimmung

Tabelle 3: Vertrauenswürdigkeitskomponenten (ASE und EAL1)

4 Geforderte Stärke der Funktionen

Die Vertrauenswürdigkeitsstufe EAL1 enthält keine Familien der Klasse AVA, insbesondere keine Komponenten der Familie AVA_SOF „Stärke der Sicherheitsfunktionen“. Postulate zur EVG-Funktionsstärke sind somit nicht erforderlich.

5 Ergebnis der Evaluierung

Der Evaluierungsendbericht [6] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Interpretationen des Schemas [4] erstellt, die für den EVG relevant sind.

Das Schutzprofil „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“ erfüllt die Anforderungen an Schutzprofile, die in den CC in der Klasse APE festgelegt sind.

Die folgende Tabelle zeigt die Ergebnisse der Evaluierung der Klasse APE:

Vertrauenswürdigkeitsklassen und Komponenten		**Urteil**
APE	**Schutzprofil-Evaluierung**	**Erfüllt**
APE_DES.1	EVG-Beschreibung	Erfüllt
APE_ENV.1	Sicherheitsumgebung	Erfüllt
APE_INT.1	PP-Einführung	Erfüllt
APE_OBJ.1	Sicherheitsziele	Erfüllt
APE_PPC.1	PP-Postulate	Erfüllt
APE_REQ.1	IT-Sicherheitsanforderungen	Erfüllt
APE_SRE.1	Explizit dargelegte IT-Sicherheitsanforderungen	Erfüllt

Tabelle 4: Vertrauenswürdigkeitskomponenten der Klasse APE

Die Evaluierung hat gezeigt, dass:

- die funktionalen Sicherheitsanforderungen für den EVG aus dem Schutzprofil konform zu Teil 2 der Common Criteria sind.

6 Definitionen

6.1 Abkürzungen

BfDI Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

BDSG Bundesdatenschutzgesetz

CC Common Criteria - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluationsgegenstand

IT Informationstechnik

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SFR Security Functional Requirement - Funktionale Sicherheitsanforderung

SOF Strength of Function - Stärke der Funktionen

ST Security Target - Sicherheitsvorgaben

TSC TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

TSF TOE Security Functions - EVG-Sicherheitsfunktionen

TSP TOE Security Policy - EVG-Sicherheitspolitik

6.2 Glossar

Zusatz - Das Hinzufügen einer oder mehrerer Vertrauenswürdigkeitskomponenten aus Teil 3 der CC zu einer EAL oder einem Vertrauenswürdigkeitspaket.

Erweiterung - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind, zu den Sicherheitsvorgaben bzw. dem Schutzprofil.

Formal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

Informell - Ausgedrückt in natürlicher Sprache.

Objekt - Eine Einheit im TSC, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG, die besondere Konsumentenbedürfnisse erfüllen.

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlaß sein muß.

Sicherheitsvorgaben - Eine Menge von Sicherheitsanforderungen und Sicherheitsspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen EVG dienen.

Semiformal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

Stärke der Funktionen - Eine Charakterisierung einer EVG-Sicherheitsfunktion, die den geringsten angenommenen Aufwand beschreibt, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrundeliegenden Sicherheitsmechanismen außer Kraft zu setzen.

SOF-Niedrig - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen angemessenen Schutz gegen zufälliges Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein geringes Angriffspotential verfügen.

SOF-Mittel - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

SOF-Hoch - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein hohes Angriffspotential verfügen.

Subjekt - Eine Einheit innerhalb des TSC, die die Ausführung von Operationen bewirkt.

Evaluationsgegenstand - Ein IT-Produkt oder -System - sowie die dazugehörigen Systemverwalter- und Benutzerhandbücher - das Gegenstand einer Prüfung und Bewertung ist.

EVG-Sicherheitsfunktionen - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfaßt, auf die Verlaß sein muß, um die TSP korrekt zu erfüllen.

EVG-Sicherheitspolitik - Eine Menge von Regeln, die angibt, wie innerhalb eines EVG Werte verwaltet, geschützt und verteilt werden.

Anwendungsbereich der TSF-Kontrolle - Die Menge der Interaktionen, die mit oder innerhalb eines EVG vorkommen können und den Regeln der TSP unterliegen.

7 Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Version 2.3, August 2005

[3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird.

[6] Evaluierungsendbericht, Version 1.1, 17.01.2007, „Evaluierungsendbericht Software zur Verarbeitung von personenbezogenen Bilddaten“, CSC Deutschland Solutions GmbH

[7] Schutzprofil BSI-PP-0023-2007 Schutzprofil „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“, 15.01.2007

Dies ist eine eingefügte Leerseite.

Anhang: Schutzprofil

Das Schutzprofil „Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0“ wird als separates Dokument zur Verfügung gestellt.